VIRGINIA IT AGENCY

DECEMBER ISOAG MEETING

VIRGINIA IT AGENCY

AGENDA

- BENJAMIN GILBERT, DHS, STRENGTHENING CYBER RESILIENCE IN A POST COVID-19 WORLD

- CHRIS JENSEN, TENABLE, PREVENTING RANSOMWARE ATTACKS

ISOAG meeting

Strengthening Cyber Resilience in a Post COVID-19 World

Benjamin Gilbert
Cybersecurity Advisor, Region III
(*Virginia, West Virginia, District of Columbia*)
Cybersecurity Advisor Program
Cybersecurity and Infrastructure Security Agency

December 2020

CISA
CYBER+INFRASTRUCTURE

CYBERSECURITY AND INFRASTRUCTURE SECURITY AGENCY

Defend Today,
Secure Tomorrow

Today's Risk Landscape

America remains at risk from a variety of threats:

- INSIDER THREAT
- ACTS OF TERRORISM
- CYBER ATTACKS
- EXTREME WEATHER
- PANDEMICS
- ACCIDENTS OR TECHNICAL FAILURES

Cyber Threats Can Cause Operational Impacts

- **Ransomware**
  - WannaCry
  - REvil/ Sodinokibi (targeting MSPs)
  - Ryuk (targeting medical, education, SLTT)
  - Robinhood, Maze, Fobos, CovidLock, CryptoLocker, ,Pysa, VoidCrypt…

- **malware**
  - Trickbot, Emotet, LokiBot
  - [wiperware] NotPetya
  - [ICS/OT specific] Triton/hatman malware targets Safety Instrumented Systems (SIS)

- **Threats to External Dependencies**
  - 3rd party vendors, service providers, infrastructure providers
  - Supply chain

Sources include: www.Malwarebytes.com
www.us-cert.cisa.gov/ics

Cyber Threats Under COVID-19

- Coronavirus Phishing Activity
- Fake Websites & Infection Tracking Sites
- Remote Access & Virtual Collaboration platforms being targeted
- Increase in Coronavirus-related Cyberattacks – particularly with healthcare manufacturing and COVID-19 related research companies

Common Vulnerabilities & Recent Exposures

- **Microsoft Netlogon Remote Protocol vulnerability** CVE-1472
- **Microsoft Exchange Server** vulnerability CVE-2020-0688
- **Citrix** vulnerability related CVE-2019-19781
- **Apache** vulnerability related to CVE-2020-1938
- **Secure VPN** vulnerability CVE-2019-11510
- **Palo Alto Networks** firewall vulnerability CVE-2020-2021
- **Microsoft DNS Server** vulnerability CVE-2020-1350
- **SAP NetWeaver** vulnerability CVE-2020-6287

Recent Alerts and Advisories

- October 30, 2020 joint CISA, FBI advisory on Iranian APT Actors Targeting Voter Registration Data
- October 28, 2020 joint CISA, HHS, FBI advisory of ransomware activity targeting Healthcare Sectors
- October 9, 2020 alert on APT actors chaining vulnerabilities against SLTT, CI, Elections Organizations
- September 15, 2020 alert on Iran-based threat actors exploiting PulseSecure, Citrix and F5 vulnerabilities
- September 14, 2020 alert by CISA/FBI on Chinese MSS targeting U.S. Government agencies
- August 2020 alert by CISA on threat actors spoofing SMA COVID-19 loan relief
- July 2020 alert by CISA/NSA recommending immediate actions to reduce exposure to OT and ICS
- April 2020 alert by CISA/NCSC on APT actors exploiting COVID-19 to target organizations
- March 2020 announcement by CISA/FBI on Chinese actors targeting COVID-19 research organization

Source: https://us-cert.cisa.gov/ncas/alerts

Protective Measures - 1

IT Security Professionals and Leadership - The Essentials (short term)

- **Inventory all technology and information assets**. Identify high-value assets, **prioritize**, and deploy controls according to criticality to the organization's operations.
- **Deploy antivirus on servers and workstations** and ensure all are up-to-date
- **Turn on logging for all network appliances, servers and services** and implement a plan for managing logs
- **Backup data regularly** using secure, well-tested and accessible solutions. Know the limitations, where data resides, and how to access when primary means start to fail
- **Implement patch management practices** that can allow for patching vulnerabilities in a timely manner, (e.g., <30 days for critical vulnerabilities, <60 days for less severe vulnerabilities, etc.)
- **Implement strong user management practices**. This includes using strong password policies, least privilege practices, and using multi-factor authentication on high-value assets.

Protective Measures - 2

IT Security Professionals and Leadership - The Essentials (longer term)

- **Have a plan for responding to cyber incidents** and **respond** to cyber incidents that are reported. Periodically review and update incident response plan accordingly.

- **Develop and strengthen situational awareness** - Sign up for membership with industry ISACs and leading cybersecurity centers and monitor for notifications and alerts.

- **Implement innovative security awareness training** as part of an incident management strategy

- **Implement a secure network architecture**. This includes ensuring properly configured network and security devices, network segmentation (or network isolation if systems are unpatchable), application and device whitelisting/blacklisting, hw/sw hardening, adoption of zero-trust models, etc.

- **Utilize cyber attack frameworks** during response and recovery of cyber attacks

- **Conduct internal audits and periodic cyber assessments** (risk-based, practice-based, and technical vulnerability assessments) in order to understand current security posture, gaps, capabilities, and operational capacities. Develop and implement mitigation plans.

Protective Measures - 3

Organizational Leaders

- Know business risks and treat cyber as a business risk, to operations and to supply chains
- Foster a culture of operational resilience and cyber readiness
- Incorporate cybersecurity as a part of business strategy, including all external relationships
- Build a network of trusted relationships with sector partners and government agencies for access to timely cyber threat information, incident reporting, and response coordination

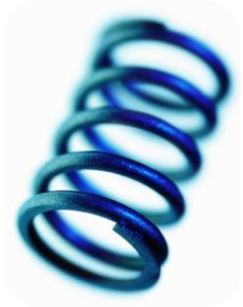
Everyone

- Participate in security awareness training and know
- Be aware of your digital footprint and know the end-user security features available to you
- Know the data backup options available and ensure locally stored data is backed up
- Be vigilant, accountable, and report incidents and suspicious activity immediately

Resilience Defined

"… the ability to prepare for and adapt to changing conditions and withstand and recover rapidly from disruptions. Resilience includes the ability to withstand and recover from deliberate attacks, accidents, or naturally occurring threats or incidents…"

- Presidential Policy Directive 21
February 12, 2013



Protect (Security)	**Sustain (Continuity)**
Perform (Capability)	**Repeat (Maturity)**

Operational Resilience in Practice

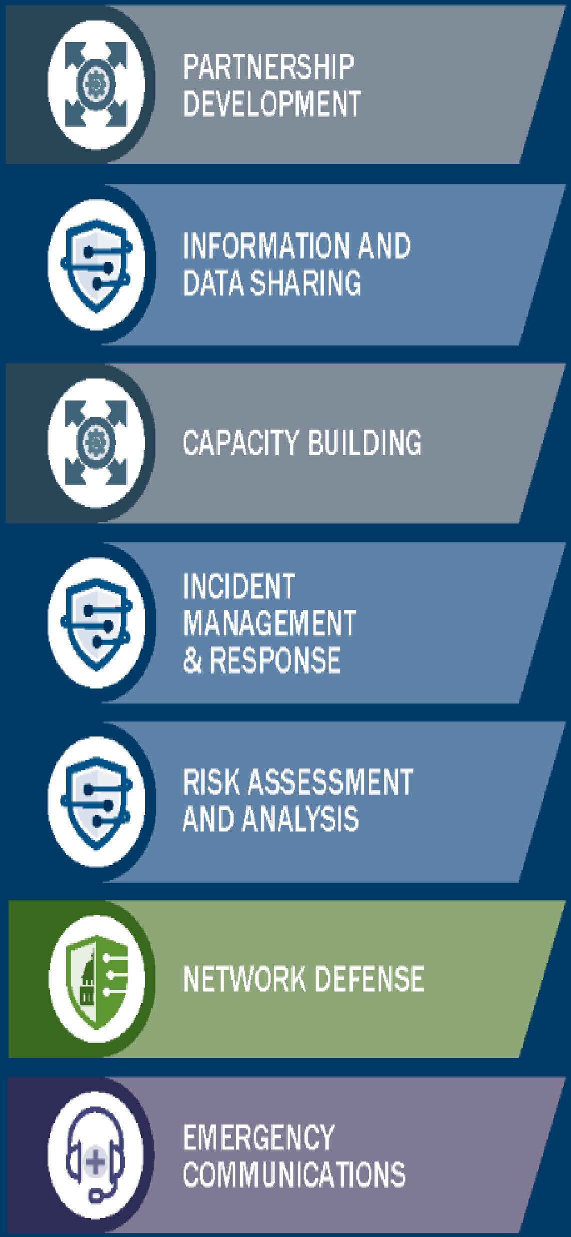
Operational resilience emerges from what we do, such as:

- Identifying and mitigating risks,
- Planning for and managing vulnerabilities and incidents,
- Performing service-continuity processes and planning,
- Managing IT operations,
- Managing, training, & deploying people,
- Protecting and securing important assets, and
- Working with external partners.

CYBERSECURITY &
INFRASTRUCTURE
SECURITY AGENCY

Who We Are

The Cybersecurity and Infrastructure Security Agency (CISA) is the Nation's risk advisor, working with partners to defend against today's threats and collaborating to build more secure and resilient infrastructure for the future



PARTNERSHIP DEVELOPMENT

INFORMATION AND DATA SHARING

CAPACITY BUILDING

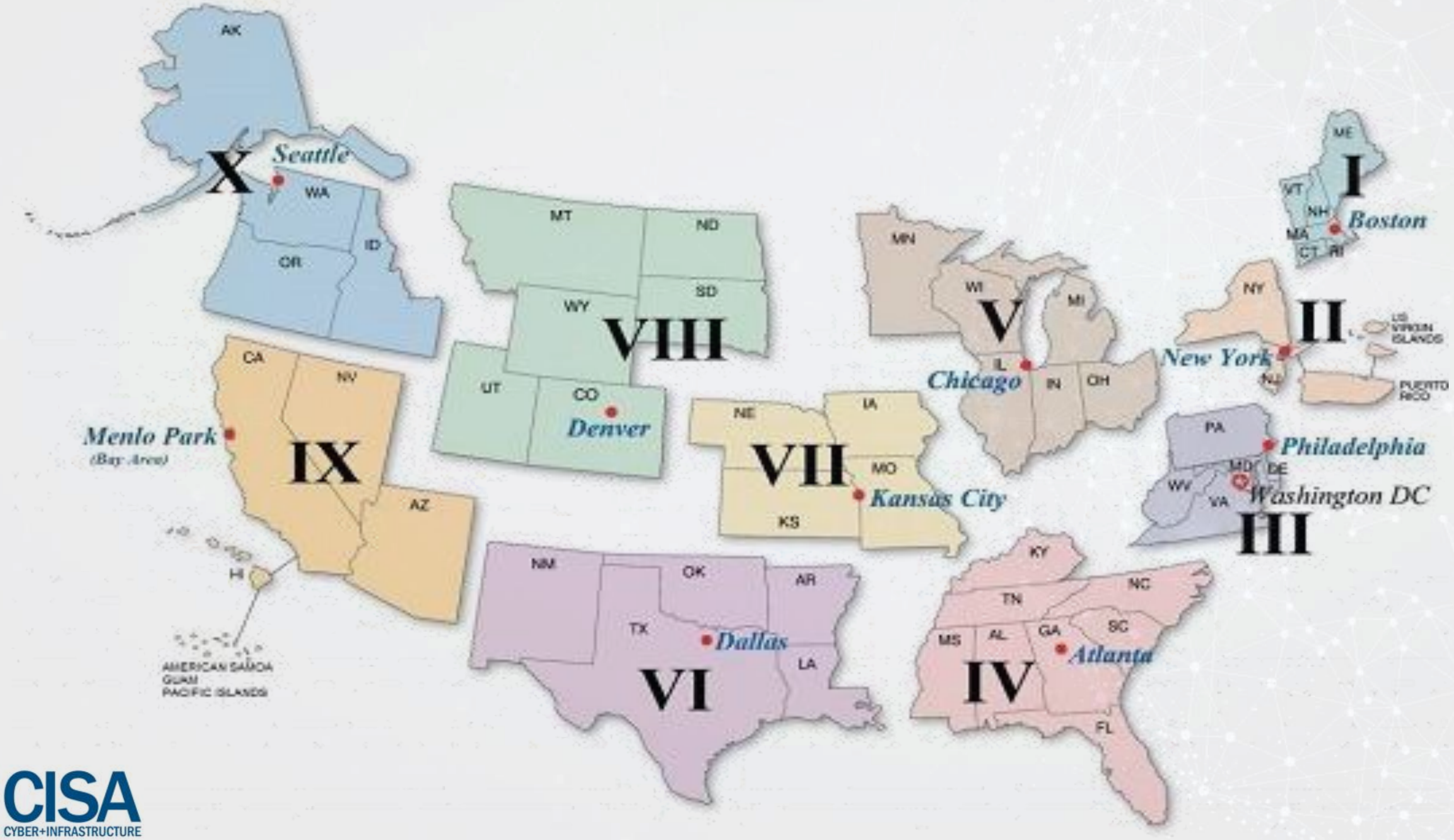
INCIDENT MANAGEMENT & RESPONSE

RISK ASSESSMENT AND ANALYSIS

NETWORK DEFENSE

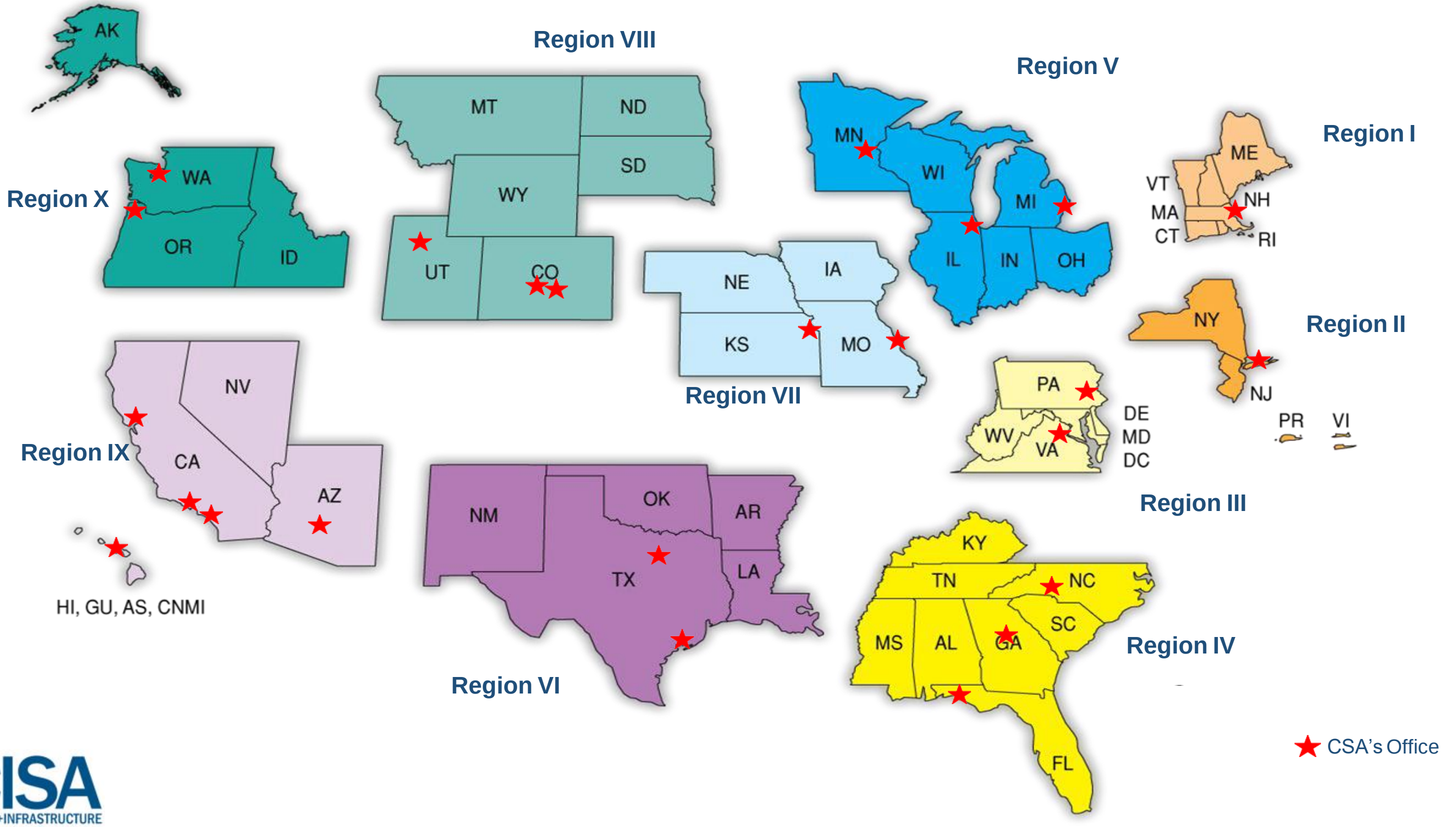
EMERGENCY COMMUNICATIONS

CISA Regions



CISA
CYBER+INFRASTRUCTURE

Cybersecurity Advisors



CISA
CYBER+INFRASTRUCTURE

CISA Offers No-Cost Cybersecurity Services

- **Preparedness Activities**
  - Cybersecurity Assessments
  - Cybersecurity Training and Awareness
  - Cyber Exercises and "Playbooks"
  - Information / Threat Indicator Sharing
  - National Cyber Awareness System
  - Vulnerability Notes Database
  - Information Products and Recommended Practices

- **Response Assistance**
  - Remote / On-Site Response and Assistance
  - Incident Coordination
  - Threat intelligence and information sharing
  - Malware Analysis

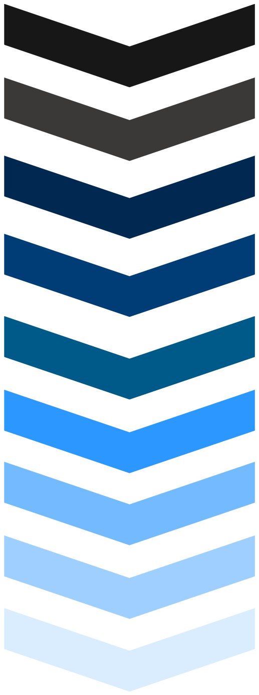
- **Cybersecurity Advisors**
  - Incident response coordination
  - Cyber assessments
  - Working group collaboration
  - Advisory assistance
  - Public Private Partnership Development

CISA
CYBER+INFRASTRUCTURE

Range of Cybersecurity Assessments

- Cyber Resilience Review (Strategic)
- External Dependencies Management (Strategic)
- Cyber Infrastructure Survey (Strategic)
- Cybersecurity Evaluations Tool Strategic (standards)
- Phishing Campaign Assessment (Tactical)
- Validated Architecture Design Review (Tactical)
- Vulnerability Scanning / Hygiene (Technical)
- Remote Penetration Test (Technical)
- Risk and Vulnerability Assessment (Technical)

STRATEGIC
(C-Suite Level)



TECHNICAL
(Network-Administrator Level)

Additional Information Sharing Opportunities

- **Multi-State Information Sharing and Analysis Center:**
  - Focal point for cyber threat prevention, protection, response and recovery for state, local, tribal, and territorial governments.
  - Operates 24 x7 cyber security operations center, providing real-time network monitoring, early cyber threat warnings and advisories, vulnerability identification and mitigation and incident response. For more information, visit www.cisecurity.org/ms-isac or email info@msisac.org
- **ISACs and ISAOs:**
  - **Information Sharing and Analysis Centers** (ISACs) or **Organizations** (ISAOs) are communities of interest sharing cybersecurity risk, threat information, and incident management to members. For more information on ISACs, visit www.nationalisacs.org. For more on ISAOs visit www.isao.org/about.

MS-ISAC®
Multi-State Information Sharing & Analysis Center®

Elections Infrastructure ISAC™

ONG-ISAC

National Defense ISAC

Real Estate ISAC Information Sharing and Analysis Center
Serving the Commercial Facilities Sector

WATER ISAC

SPACE ISAC

Maritime Transportation System Information Sharing and Analysis Center

REN-ISAC

RETAIL & HOSPITALITY ISAC

DNG-ISAC

H-ISAC HEALTH - ISAC

CISA CYBER+INFRASTRUCTURE

M-E ISAC MEDIA + ENTERTAINMENT INFORMATION SHARING ANALYSIS CENTER

FS-ISAC

IT ISAC

E-ISAC ELECTRICITY INFORMATION SHARING AND ANALYSIS CENTER

AUTO-ISAC Automotive Information Sharing and Analysis Center

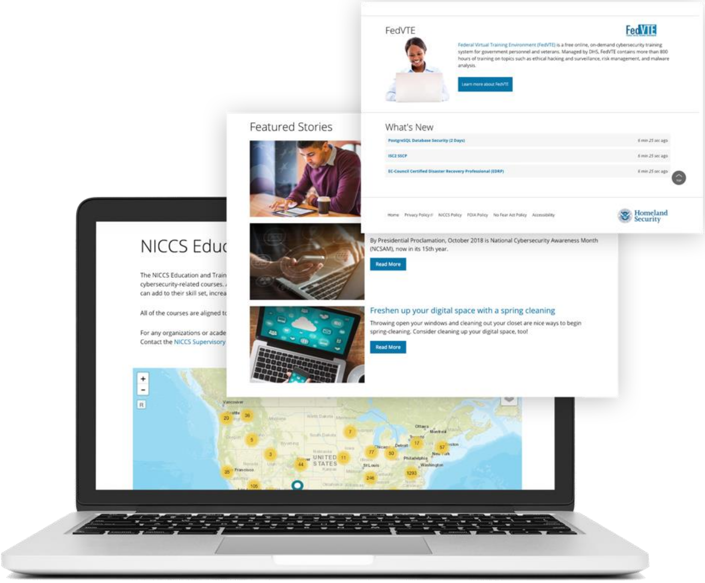
AVIATION ISAC

Cybersecurity Training Resources

CISA offers easily accessible education and awareness resources through the National Initiative for Cybersecurity Careers and Studies (NICCS) website.

The NICCS website includes:

- Searchable Training Catalog with 4,400 plus cyber-related courses offered by nationwide cybersecurity educators
- Interactive National Cybersecurity Workforce Framework
- Cybersecurity Program information: **FedVTE**, Scholarships for Service, Centers for Academic Excellence, and Cyber Competitions
- Tools and resources for cyber managers
- Upcoming cybersecurity events list



NICCS Educ

The NICCS Education and Train
cybersecurity-related courses.
can add to their skill set, increa

All of the courses are aligned t

For any organizations or acade
Contact the NICCS Supervisory

Featured Stories

By Presidential Proclamation, October 2018 is National Cybersecurity Awareness Month (NCSAM), now in its 15th year.

Read More

Freshen up your digital space with a spring cleaning

Throwing open your windows and cleaning out your closet are nice ways to begin spring-cleaning. Consider cleaning up your digital space, too!

Read More

FedVTE

Federal Virtual Training Environment (FedVTE) is a free online, on-demand cybersecurity training system for government personnel and veterans. Managed by DHS, FedVTE contains more than 800 hours of training on topics such as ethical hacking and surveillance, risk management, and malware analysis.

Learn more about FedVTE

What's New

PostgreSQL Database Security (2 Days)	6 min 25 sec ago
ISC2 SSCP	6 min 25 sec ago
EC-Council Certified Disaster Recovery Professional (EDRP)	6 min 25 sec ago

Home Privacy Policy NICCS Policy FOIA Policy No Fear Act Policy Accessibility

CISA
CYBER+INFRASTRUCTURE

For more information, visit NICCS.US-CERT.gov

Federal Response to Significant Cyber Incidents

PPD 41: United States Cyber Incident Coordination

Sets forth principles governing the Federal response to cyber incidents that significantly impact a public or private sector entity, national security, or the economy

Threat Response

Law enforcement and national security investigative activities

FBI and National Cyber Investigative Joint Task Force (Department of Justice)

Asset Response

Technical assistance, mitigation, risk assessment

Cybersecurity and Infrastructure Security Agency (Department of Homeland Security)

Intelligence

Intelligence Support

Cyber Threat Intelligence Integration Center

(Office of the Director of National Intelligence)

CISA
CYBER+INFRASTRUCTURE

Response Assistance- CISA Central

CISA Central– Federal government’s premier all-hazards watch floor

** Formerly known as the National Cybersecurity & Communications Integration Center (NCCIC), *[AFKA., CISA Integrated Operations Coordination Center (C-IOCC)*]

Works to reduce the risk of systemic cybersecurity and communications challenges.

Core cybersecurity efforts include:

- **Operations**
  - 24/7 Watch operations
    - ICS/US-CERT, ISACs, LNOs ,IC
  - Threat Hunting and Incident response
- **Cyber Threat Detection and Analysis**
  - Data synthesis and analysis
  - 24/7 malware analysis lab
  - Threat intelligence and Information exchange

CISA
CYBER+INFRASTRUCTURE

Contact CISA to report a cyber incident

Call 1-888-282-0870 | email CISAservicedesk@cisa.dhs.gov | visit https://www.cisa.gov

Cyber Incident Reporting

When to Report:

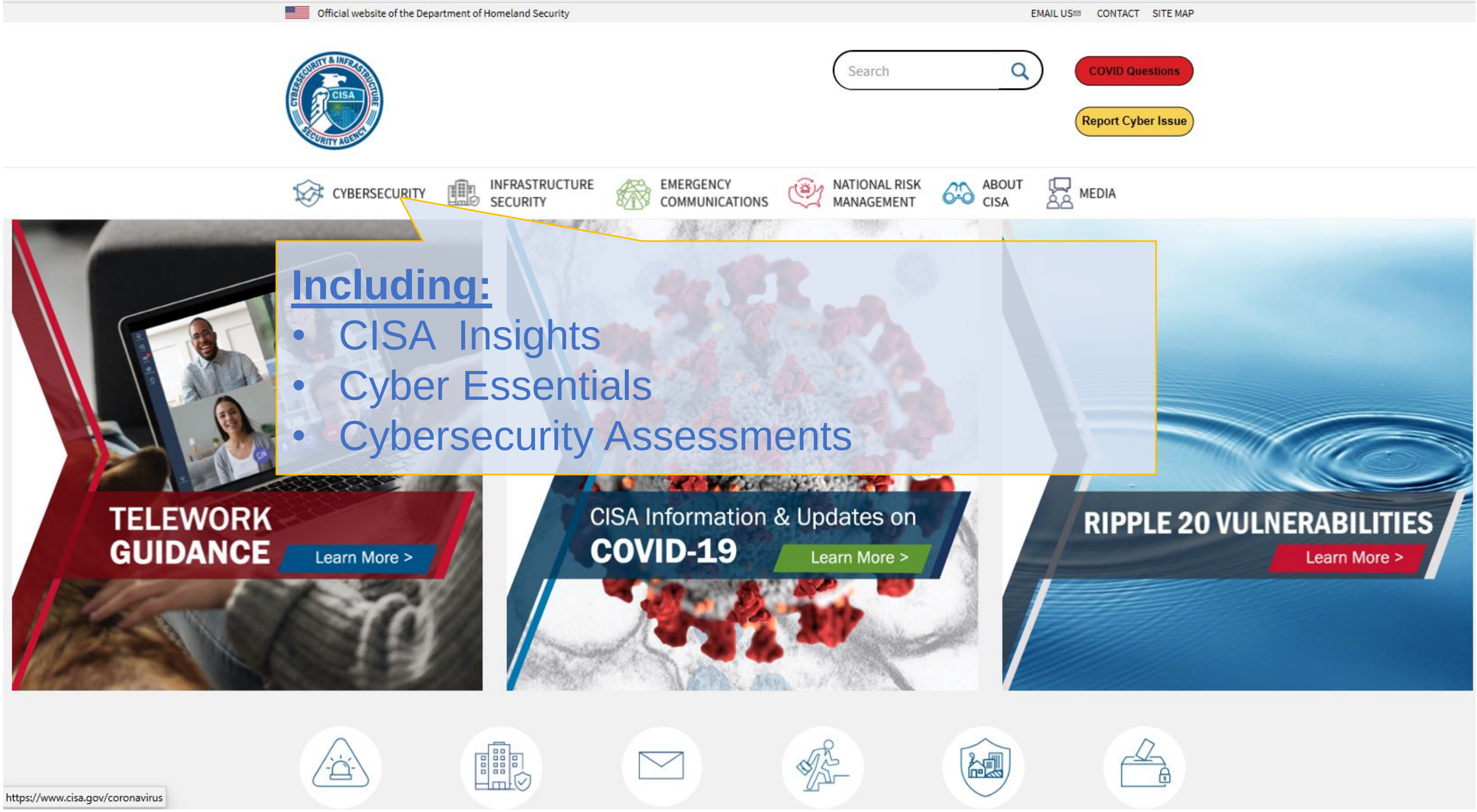
If there is a suspected or confirmed cyber attack or incident that:

- Affects core government or critical infrastructure functions;
- Results in the loss of data, system availability; or control of systems;
- Indicates malicious software is present on critical systems

Virginia Fusion Center (VFC)

Cyber Intelligence Unit:
VFC : (804)-674-2196
vfccyber@vsp.virginia.gov

https://www.cisa.gov



Including:

- CISA Insights
- Cyber Essentials
- Cybersecurity Assessments

Contact CISA

Questions???

CISA
CYBER+INFRASTRUCTURE

General Inquiries	
CISARegion3@hq.dhs.gov cyberadvisor@hq.dhs.gov	

CISA Contact Information	
Benjamin Gilbert **Cybersecurity Advisor, Region III** **(VA, WV, DC)** **Rob Mooney, SPSA, Eastern VA** **Jamie Finney, PSA, Western VA**	Benjamin.gilbert@hq.dhs.gov Robert.Mooney@cisa.dhs.gov James.Finney@hq.dhs.gov
Reporting Cyber Incidents to CISA	**1-888-282-0870** CISAservicedesk@cisa.dhs.gov https://www.cisa.gov

Cybersecurity and Infrastructure Security Agency

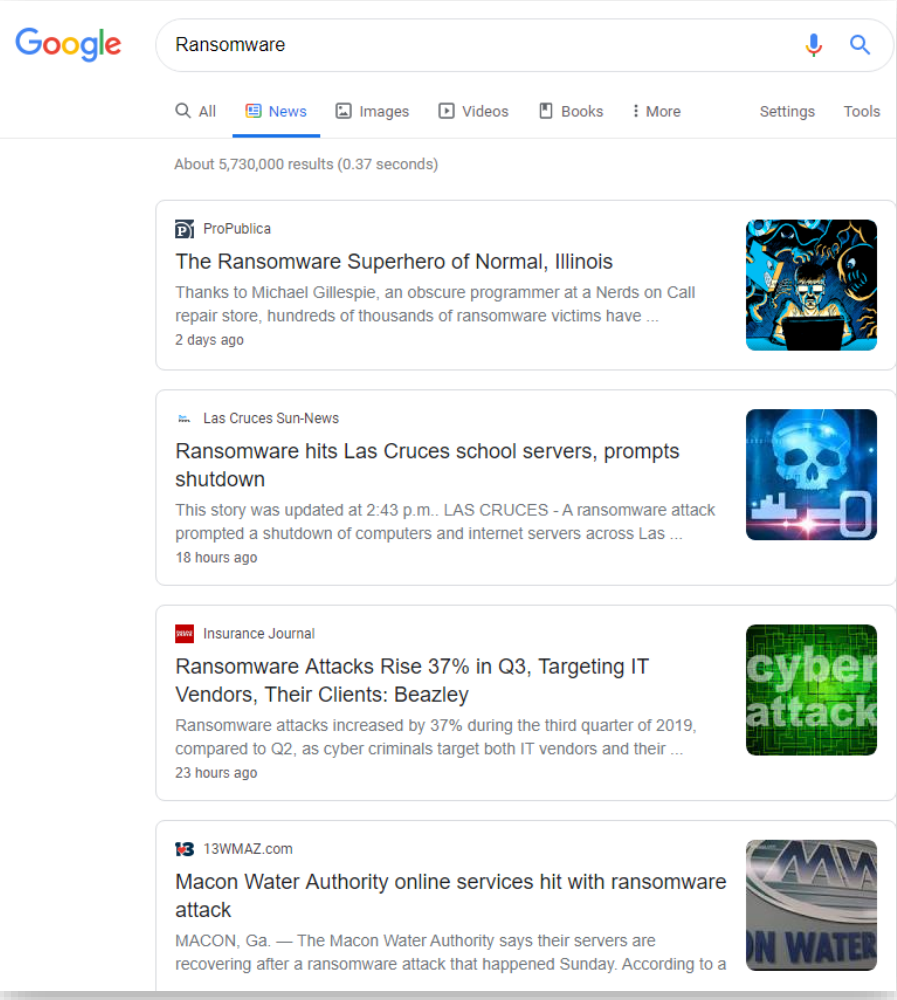
Defending against Ransomware Attacks with Risk-Based Vulnerability Management

Chris Jensen

Public Sector Business Development

VITA ISOAG Meeting

Dec. 2, 2020



About 5,730,000 results (0.37 seconds)

ProPublica

The Ransomware Superhero of Normal, Illinois

Thanks to Michael Gillespie, an obscure programmer at a Nerds on Call repair store, hundreds of thousands of ransomware victims have ...

2 days ago

Las Cruces Sun-News

Ransomware hits Las Cruces school servers, prompts shutdown

This story was updated at 2:43 p.m.. LAS CRUCES - A ransomware attack prompted a shutdown of computers and internet servers across Las ...

18 hours ago

Insurance Journal

Ransomware Attacks Rise 37% in Q3, Targeting IT Vendors, Their Clients: Beazley

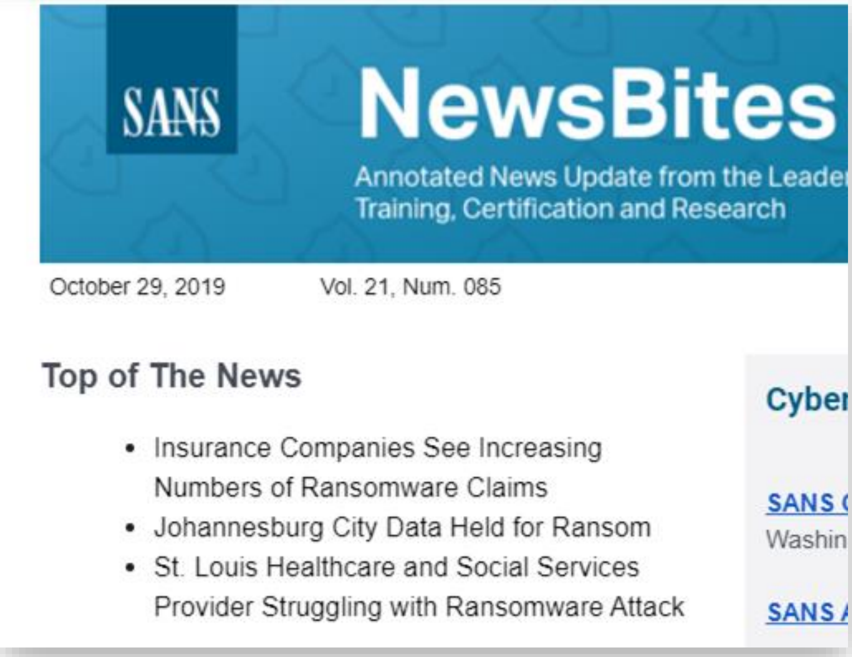
Ransomware attacks increased by 37% during the third quarter of 2019, compared to Q2, as cyber criminals target both IT vendors and their ...

23 hours ago

13WMAZ.com

Macon Water Authority online services hit with ransomware attack

MACON, Ga. — The Macon Water Authority says their servers are recovering after a ransomware attack that happened Sunday. According to a



SANS
NewsBites
Annotated News Update from the Leade
Training, Certification and Research

October 29, 2019 Vol. 21, Num. 085

Top of The News

- Insurance Companies See Increasing Numbers of Ransomware Claims
- Johannesburg City Data Held for Ransom
- St. Louis Healthcare and Social Services Provider Struggling with Ransomware Attack

Cyber

SANS

Washin

SANS

PREVENTION VS. CURE

- Complete ransomware protection is multi-phased:
  - Preventing attacks
  - Backing up data to minimize damage from an attack
  - Building in resiliency to recover quickly from an attack

- This briefing focuses on prevention

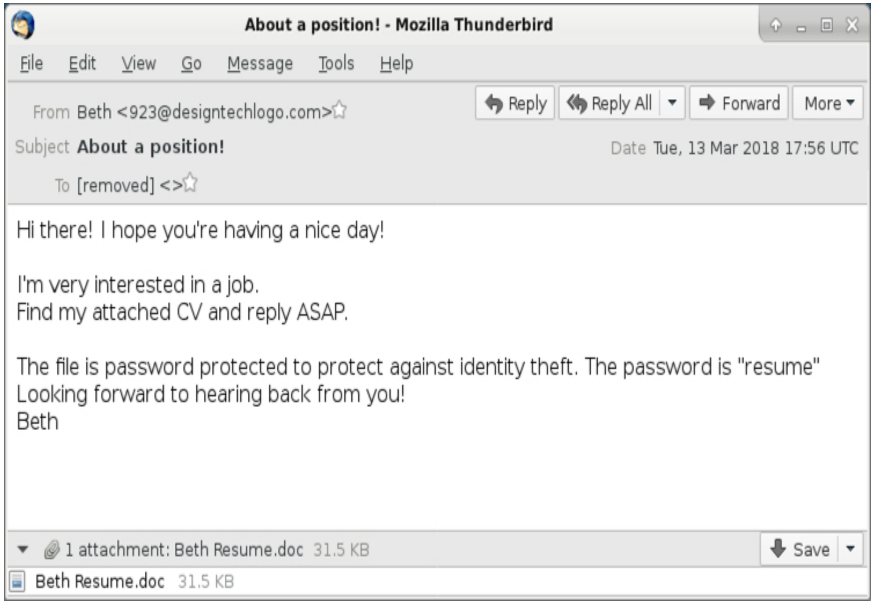
tenable®

DEFENDING YOUR NETWORK “HOME”

- Hackers are not specifically targeting you; they are looking for easy targets
- Local governments are appealing targets in general – lots of valuable PII, but limited budgets and resources
- It’s a big neighborhood (over 75,000 local government entities in the US)
- Be the hard target; send hackers to a softer target down the street

Ransomware Infection Techniques

Malicious Emails – Opening the Door



From Beth <923@designtechlogo.com>

Subject **About a position!**

Date Tue, 13 Mar 2018 17:56 UTC

To [removed] <>

Hi there! I hope you're having a nice day!

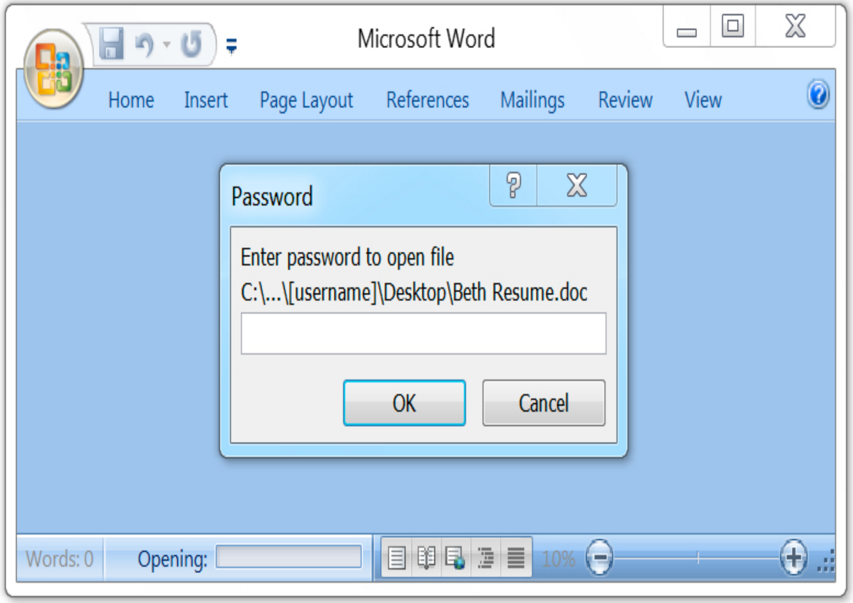
I'm very interested in a job.
Find my attached CV and reply ASAP.

The file is password protected to protect against identity theft. The password is "resume"
Looking forward to hearing back from you!
Beth

1 attachment: Beth Resume.doc 31.5 KB

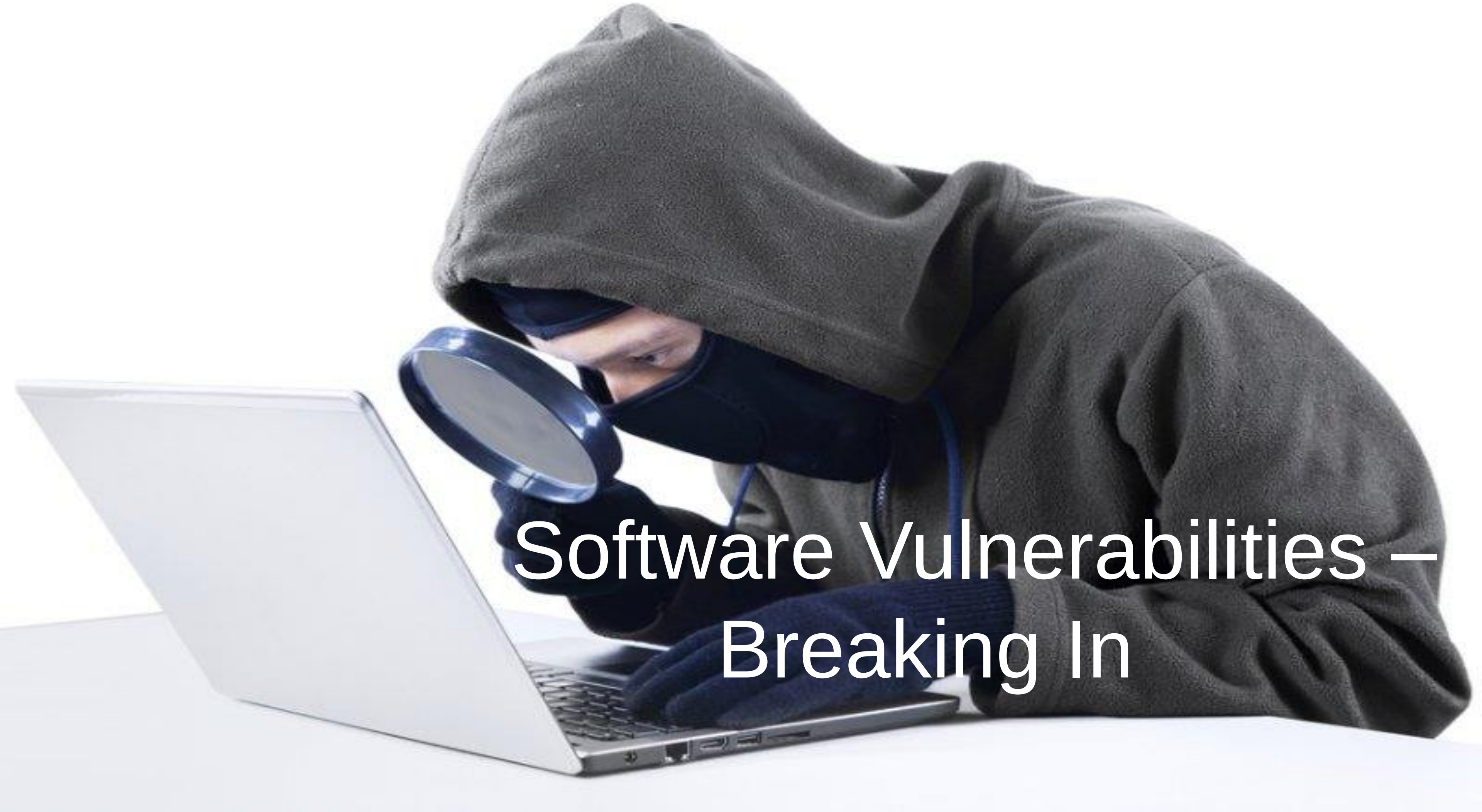
Beth Resume.doc 31.5 KB

Beth
Resume.doc



Enter password to open file
C:\...\[username]\Desktop\Beth Resume.doc

Bruteforce – Exploiting weak locks



Software Vulnerabilities – Breaking In

DARKReading

9/26/19

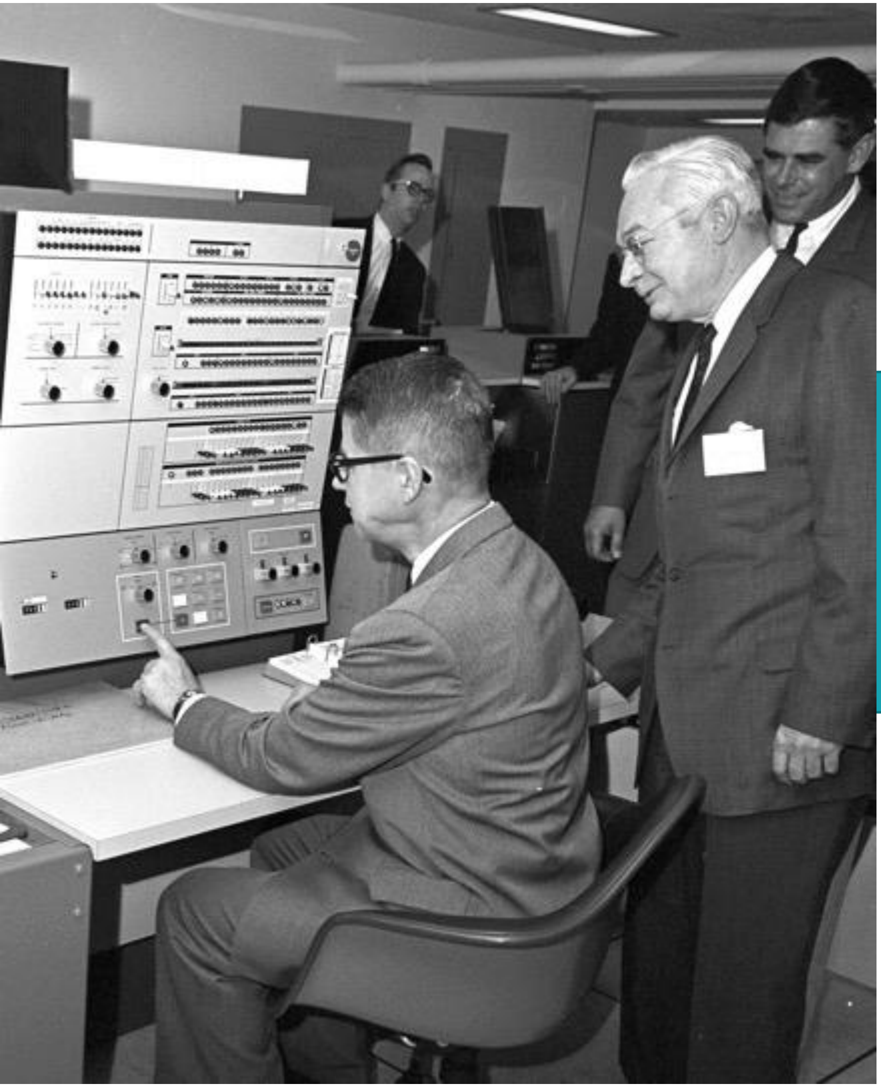
Ransomware Hits Multiple, Older Vulnerabilities

Ransomware attacks are taking advantage of vulnerabilities that are older and less severe, a new report finds.

Ransomware attacks are taking advantage of vulnerabilities that might have gone unnoticed by security teams, with more than half of exploited vulnerabilities having a CVSS v2 score less than 8.

This 2019 report found that **35% of the vulnerabilities exploited in ransomware attacks were more than 3 years old**.

Source: https://www.darkreading.com/vulnerabilities---threats/ransomware-hits-multiple-older-vulnerabilities-/d/d-id/1335930



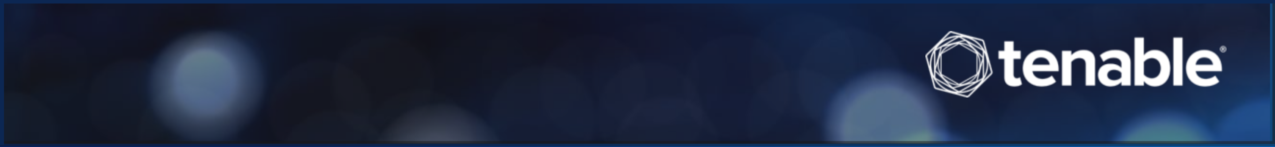
Legacy Vulnerability Management Can’t Keep Up

- Limited Visibility
- Ineffective Prioritization
- Poor Risk Communication

Legacy Tools Can’t Handle The Modern Attack Surface

Upgrade to Risk-based Vulnerability Management

- See the full attack service
- Eliminate vulnerability overload
- Measure risk, not vulnerabilities

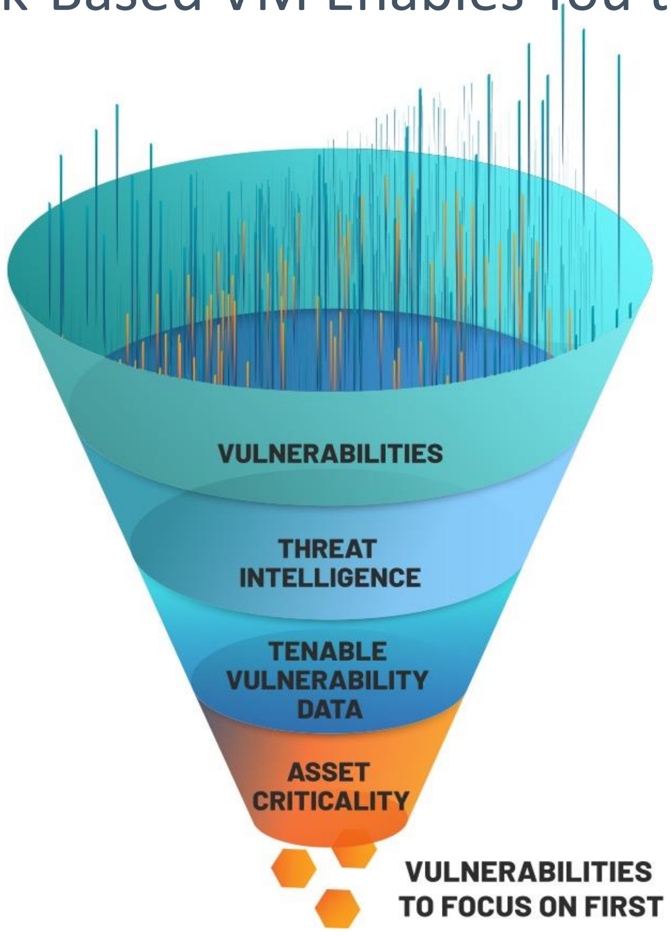


A process that employs machine learning analytics
to automatically correlate:

- **Assessments of traditional and modern assets across the entire attack surface**
- **Vulnerability severity**
- **Threat and exploit intelligence**
- **Asset criticality**

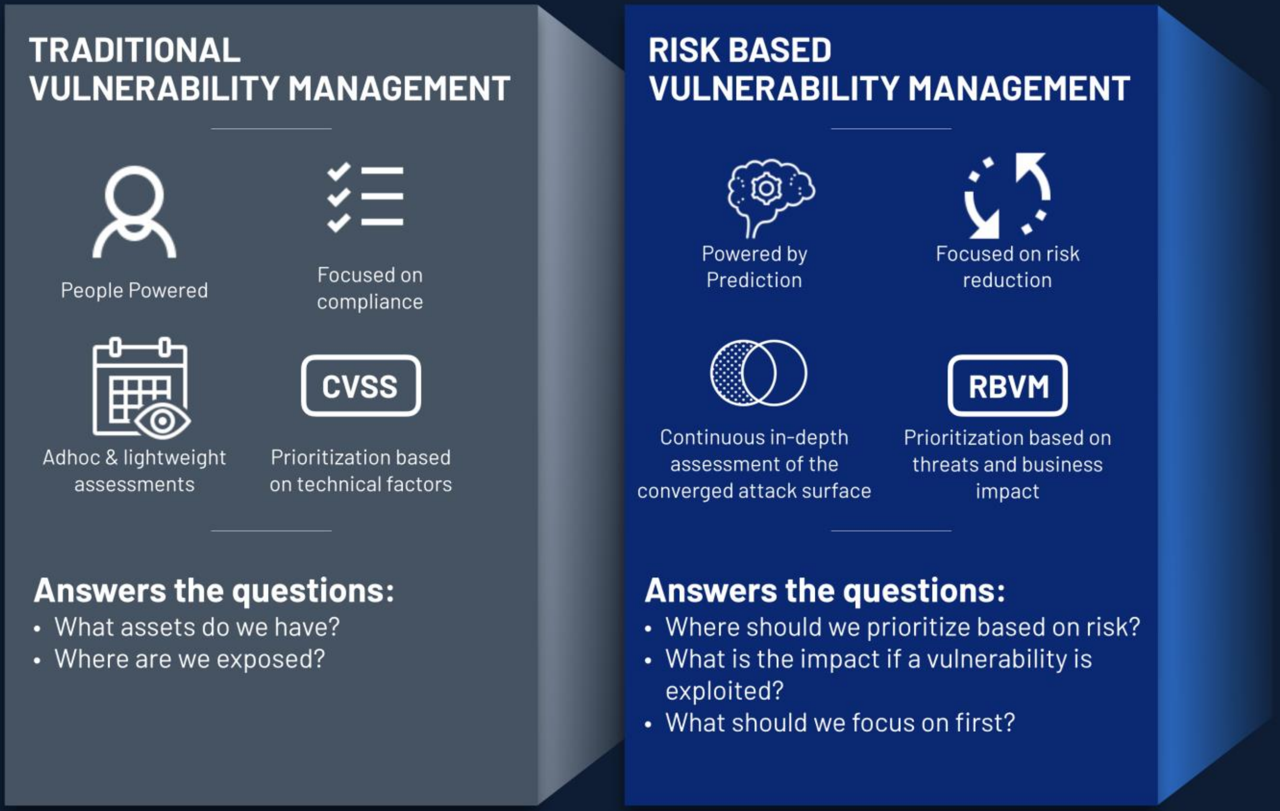
… to identify which vulnerabilities pose the greatest risk.

Risk-Based VM Enables You to Focus First on What Matters Most



- Address your **entire** attack surface
- Understand vulnerabilities in the **context** of risk
- **Stop** wasting time on vulnerabilities that don’t pose risk
- Reduce the greatest amount of business **risk** with the least amount of effort

From **Vulnerability Management** to **Risk Based VM**



TRADITIONAL VULNERABILITY MANAGEMENT

People Powered

Focused on compliance

Adhoc & lightweight assessments

CVSS

Prioritization based on technical factors

Answers the questions:

- What assets do we have?
- Where are we exposed?

RISK BASED VULNERABILITY MANAGEMENT

Powered by Prediction

Focused on risk reduction

Continuous in-depth assessment of the converged attack surface

RBVM

Prioritization based on threats and business impact

Answers the questions:

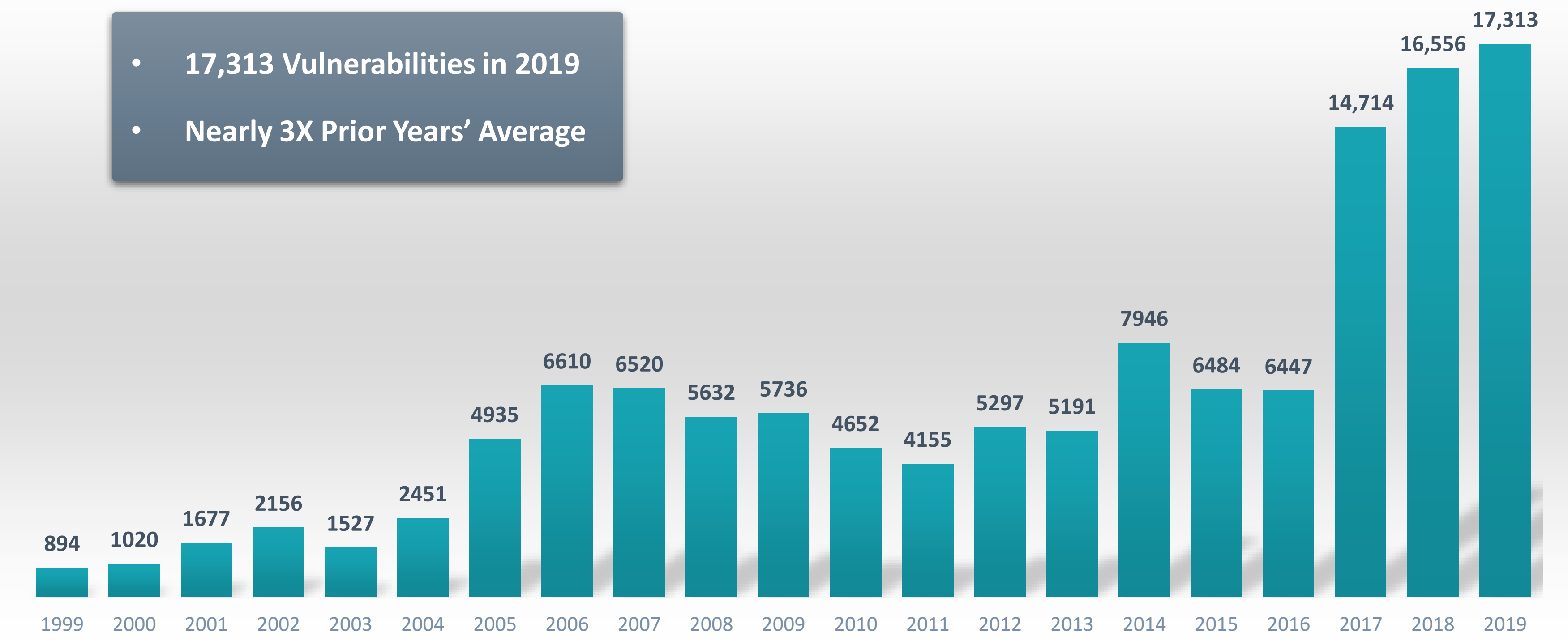
- Where should we prioritize based on risk?
- What is the impact if a vulnerability is exploited?
- What should we focus on first?

tenable®

VM		RBVM
Compliance Driven	→	Risk Driven
Infrastructure/IT Focus	→	Expansion to Apps & Modern Assets
Static, Point in Time Visibility	→	Dynamic, Continuous Visibility
Policies & Audit Support	→	Prioritization & Strategic Decision Support
Reactive	→	Proactive
Vulnerability Data Only	→	Vuln Data Correlated w/ Threat Intelligence & Asset Criticality

The Number of New Vulnerabilities Continues to Grow

- 17,313 Vulnerabilities in 2019
- Nearly 3X Prior Years' Average



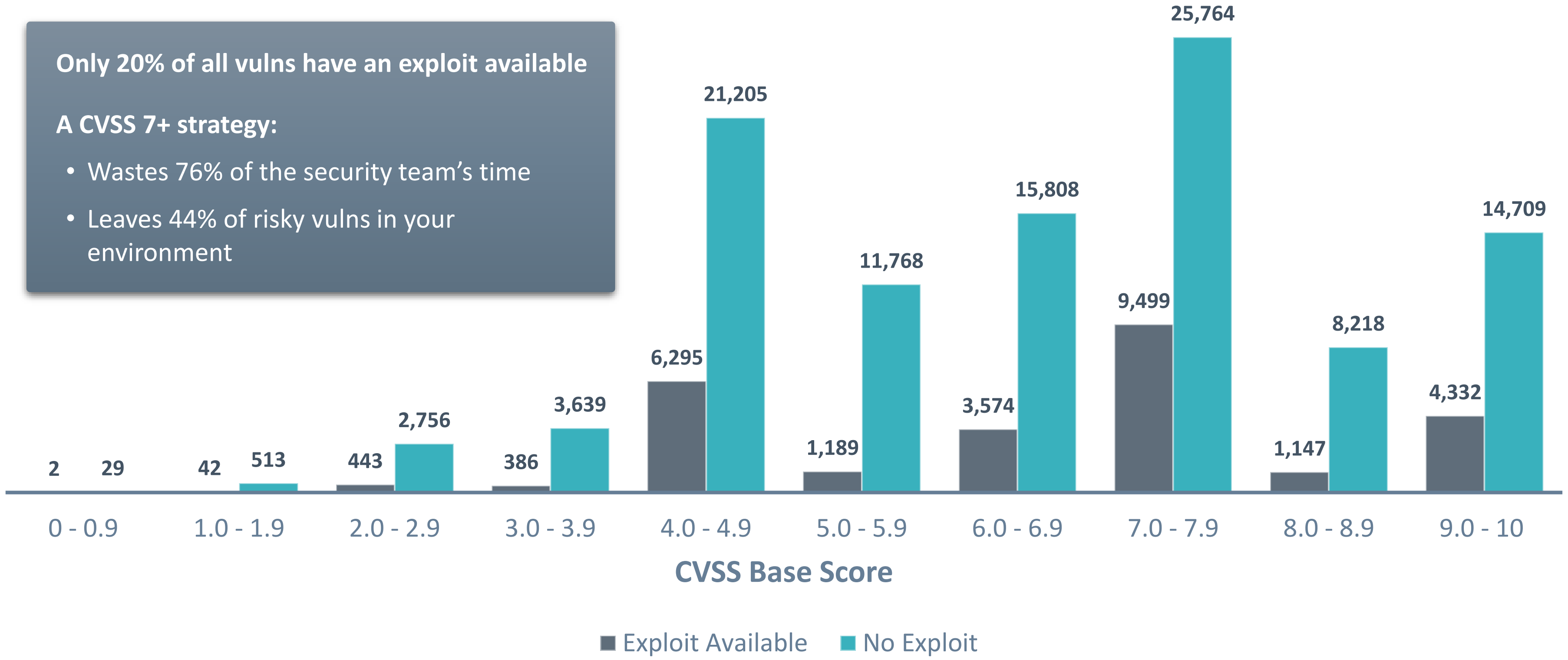
Source: Vulnerability Intelligence Report, Tenable Research

CVSS is a Poor Indicator of Risk

Only 20% of all vulns have an exploit available

A CVSS 7+ strategy:

- Wastes 76% of the security team's time
- Leaves 44% of risky vulns in your environment



Source: Tenable Research

CVSS is Heavily Flawed

"CVSS is designed to identify the technical severity of a vulnerability. What people seem to want to know, instead, is the risk a vulnerability or flaw poses to them, or ***how quickly they should respond to a vulnerability***."

TOWARDS IMPROVING CVSS

SOFTWARE ENGINEERING INSTITUTE | CARNEGIE MELLON UNIVERSITY

December 2018

17300+

VULNERABILITIES DISCLOSED IN 2019

31%

Of vulnerabilities disclosed in 2019 were rated critical or high.

Over 5,300 Vulnerabilities

13%

Of vulnerabilities disclosed in 2019 were CVSS 9+

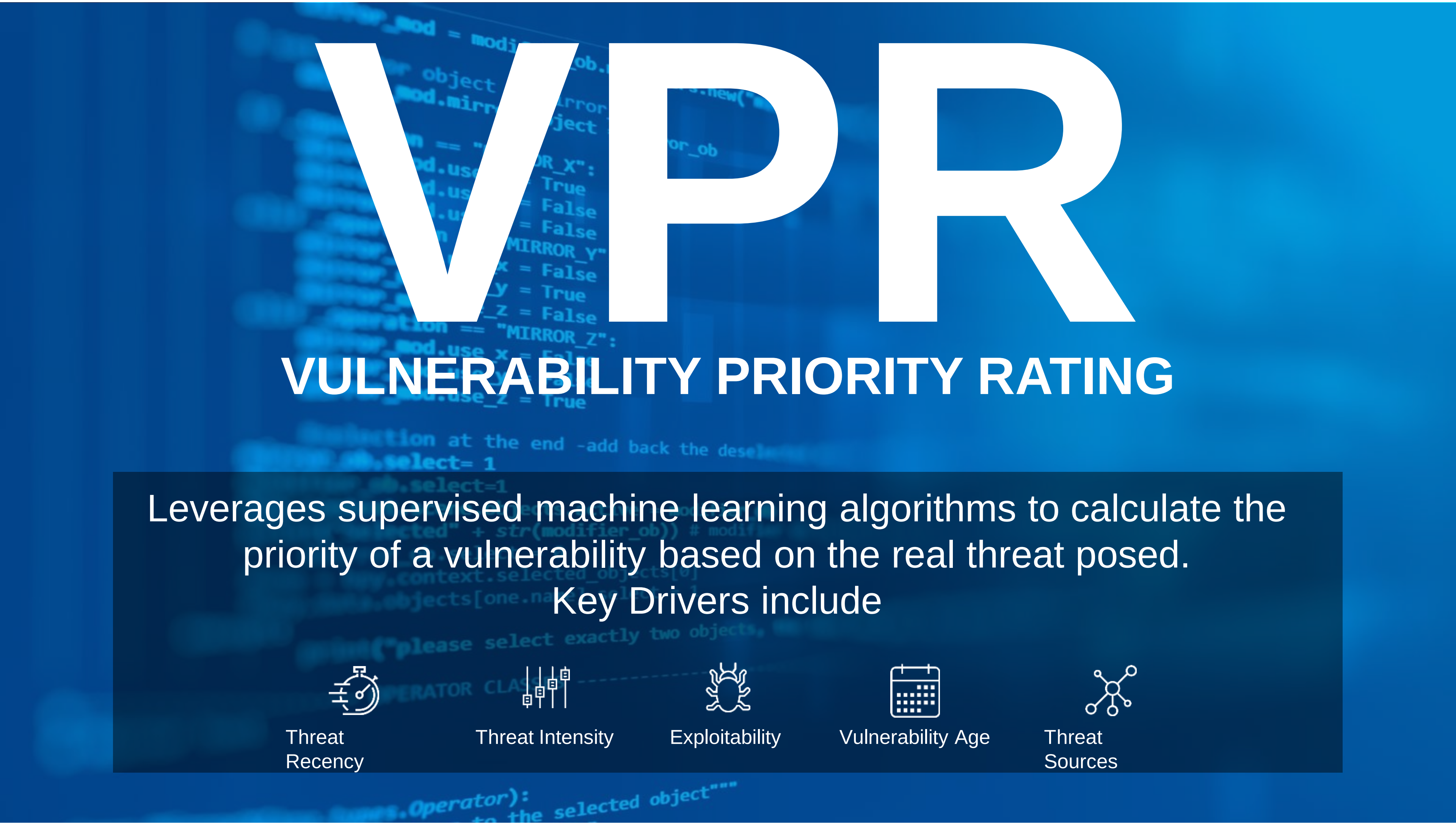
Over 2,200 Vulnerabilities

47%

Of vulnerabilities disclosed had publicly available exploits

Over 8,000 Vulnerabilities

tenable



VPR

VULNERABILITY PRIORITY RATING

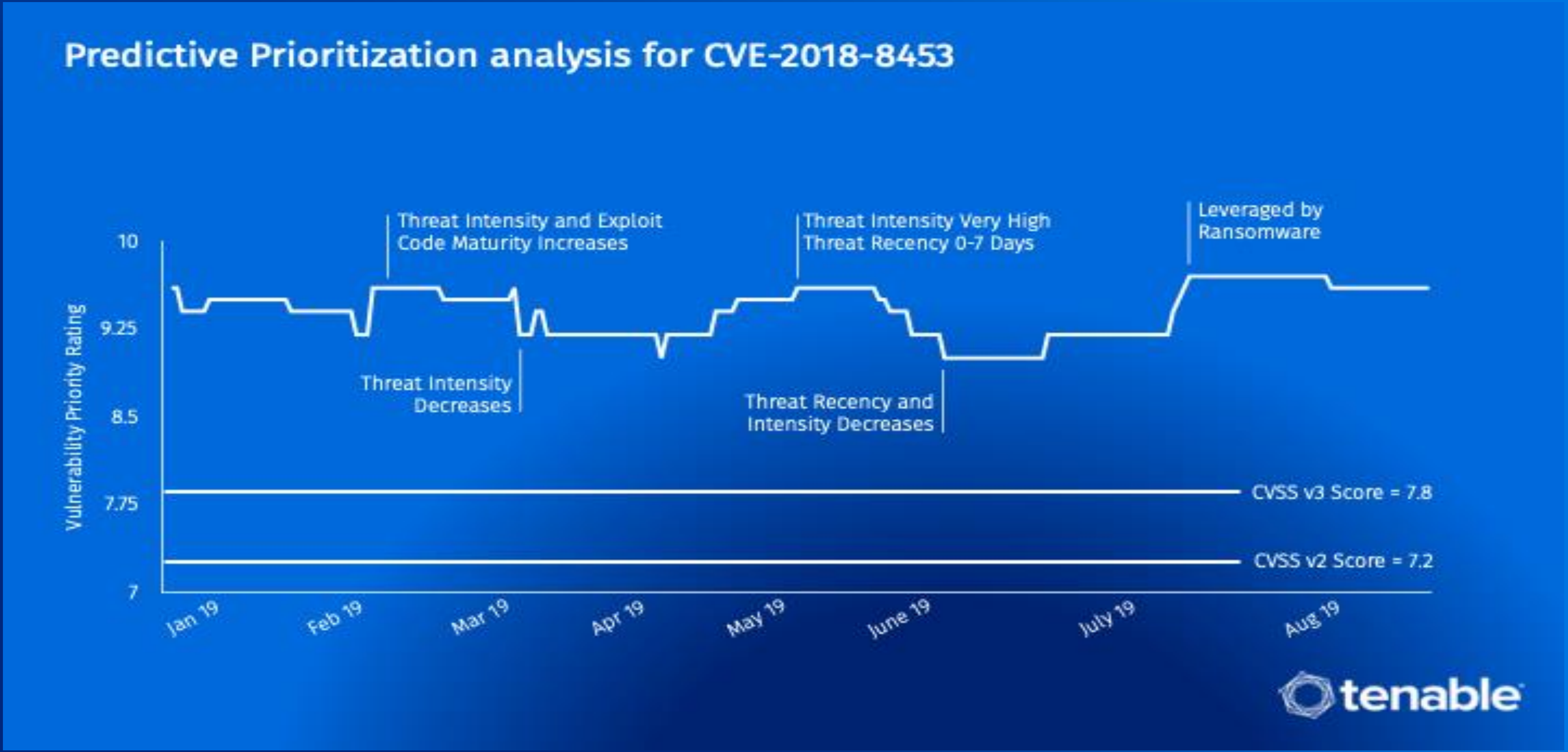
Leverages supervised machine learning algorithms to calculate the priority of a vulnerability based on the real threat posed.

Key Drivers include

- Threat Recency
- Threat Intensity
- Exploitability
- Vulnerability Age
- Threat Sources

tenable

Elevation of privilege vulnerability in Windows
Used in 2019 SLG ransomware attacks



Predictive Prioritization analysis for CVE-2018-8453

Threat Intensity and Exploit Code Maturity Increases

Threat Intensity Decreases

Threat Intensity Very High Threat Recency 0-7 Days

Threat Recency and Intensity Decreases

Leveraged by Ransomware

CVSS v3 Score = 7.8

CVSS v2 Score = 7.2

ACR

ASSET CRITICALITY RATING

Leverages algorithms to calculate the criticality of an asset to focus prioritization efforts.

Key drivers include

- Business Purpose
- Device Type
- Connectivity
- Capabilities
- Location
- 3rd Party Data

FOCUS FIRST ON WHAT MATTERS MOST

VPR

VULNERABILITY PRIORITY RATING

Leverage machine learning and threat intelligence to prioritize vulnerabilities based on likelihood of exploitation

+

ACR

ASSET CRITICALITY RATING

Prioritize assets based on the indicators of business value and impact

=

CES

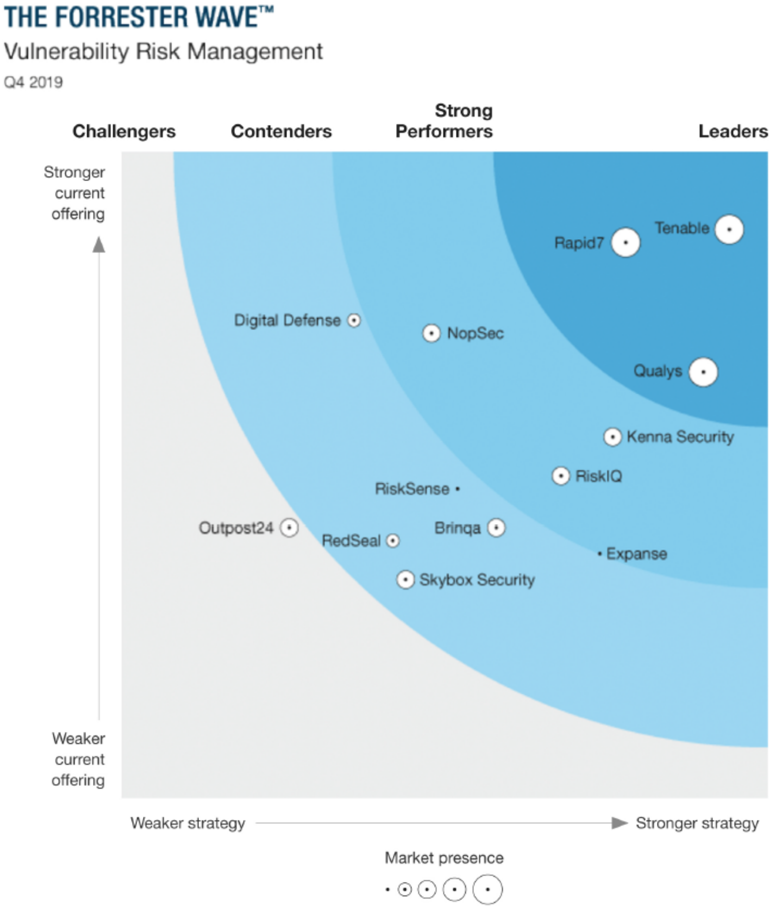
CYBER EXPOSURE SCORE

Objectively measure the Cyber Risk of an asset, business unit or whole organization

tenable

FORRESTER®

"Tenable executes on its vision to build the **single-source-of-truth platform for VRM.** Part of Tenable's strong strategy relies on **translating data to provide business insight** to provide prioritization."



tenable®

Thank you

UPCOMING EVENTS

JANUARY 2021 ISOAG

January ISOAG Meeting
Jan. 6, 2021 - 1 to 4 p.m.
Webex

- Bryan Carnahan, Assura Inc
- Dan Han, VCU
- Robert Kulak, Fire Eye

IS ORIENTATION

IS Orientation

Dec. 9 at 1p.m.

Presenter: Marlon Cole

Registration link:

https://covaconf.webex.com/covaconf/onstage/g.php?MTID=e376010e5a8341c8fd6133acaaddeaf2d

VIRGINIA
IT AGENCY

ADJOURN

THANK YOU FOR ATTENDING